UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/561,276	07/17/2006	Marc Joye	032326-314	5693

21839 7590 12/30/2009

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
12/30/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/561,276	JOYE, MARC	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on December 19, 2005. Claims 1-20 are currently being considered.

Priority

Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) - (d) is acknowledged.

Information Disclosure Statement

Applicant's IDS form 1449, received on 12/19/2005, has been considered and an initialed copy is attached to this Office action.

Drawings

The subject matter of this application admits of illustration by a drawing to facilitate understanding of the invention (refer paragraph 0089 and 0098). Applicant is required to furnish a drawing under 37 CFR 1.81(c). No new matter may be introduced in the required drawing. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d).

Specification

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Objections

Claims 2-20 objected to because of the following informalities: Typing error. Claims 2-7, and 9-17: "A countermeasure method" and Claims 8, and 17-20: "An electronic component". Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claims 1-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Applicant's claims 1-20 are directed towards an algorithm method that can be performed via physical computation using a piece of paper and pencil. The Office's current position is that such claims involving a algorithm method with functional descriptive material, do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 3, 4, and 5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner contends claims 3, 4, and 5 are improper claims on the basis that the meets and bounds of the claims cannot be readily ascertained. For example, applicant's claims recites "Let (d.sub.1(t),d.sub.1(t-1), . . . , d.sub.1(0)) and (d.sub.2(t),d.sub.2(t-

1), . . . , d.sub.2(0)))". The Examiner contends that one of ordinary skill in the art cannot reasonably identify an appropriate input bound. The Examiner maintains the same assertion for the remaining claim limitation elements. The applicant is advised to re-write the claim in a form that would allow a clear and concise understanding of the meets and bounds of the claim limitations. For example the claim may read, "an input consisting of integer value d". .

3. Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 2 claims that group G is written in *additive notation*, yet in the independent claim 1, which claims 2 depends from, the group G is written in *multiplicative notation*. This seems inconsistent and therefore renders the claim indefinite.

4. Claim 8, and 17-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 8, and 17-20 claims "An electronic component implementing the method…". This is not clear, what does it mean? Disclosure is silent regarding this specific component.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1-20 is rejected under 35 U.S.C. 102(e) as being anticipated by Clavier et al. (U.S. Patent 7,085,378).

1. Regarding Claim 1 Clavier reach and describe countermeasure method performed in an electronic component and implementing a public-key cryptography algorithm utilizing exponentiation computation of the type y=g d, where g and y are elements of a determined group G written in multiplicative notation, and d is a predetermined number, said countermeasure method comprising a masking first step for expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, and a second step for computing the value of y=g d in G by any double exponentiation algorithm of the type (g d.sub.1)(h d.sub.2) with h=g s in G (col.8 line 19 to col.9 line 30, and col.10 line 25 to col.11 line 46).

3. Claims 2-20 are rejected applied as above rejecting Claim 1. Furthermore, Clavier teach and describe a countermeasure method, wherein:

As per Claim 2, the group G is written in additive notation (col.9 line 30 tocol.10 line 22).

As per Claim 3, the method comprises the following steps: 1) Masking of d: 1a) Express d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers 1b) Let (d.sub.1(t),d.sub.1(t-1), . . . , d.sub.1(0)) and (d.sub.2(t),d.sub.2(t-1), . . . , d.sub.2(0)) be the respective binary representations of d.sub.1 and of d.sub.2 2) Double exponentiation: 2a) Define (compute) the element h=g s in G 2b) Initialize the register A with the neutral element of G 2c) For i from t down to 0, do the following: 2c1) Replace A with A 2 2c2) If d.sub.1(i)=1, replace A with Ag 2c3) If d.sub.2(i)=1, replace A with Ah 2c4) Return A (col.9 line 7 tocol.10 line 22).

As per Claim 4, the method comprises the following steps: 1) Masking of d: 1a) Express d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers 1b) Let

(d.sub.1(t),d.sub.1(t-1), . . . , d.sub.1(0)) and (d.sub.2(t),d.sub.2(t-1), . . . , d.sub.2(0)) be the respective binary representations of d.sub.1 and of d.sub.2 2) Double exponentiation: 2a) Define (compute) the element h=g s in G 2b) Precompute u=gh in G 2c) Initialize the register A with the neutral element of G 2d) For i from t down to 0, do the following: 2d1) Replace A with A 2 2d2) If d.sub.1(i)=1 and d.sub.2(i)=0, replace A with Ag 2d3) If d.sub.1(i)=0 and d.sub.2(i)=1, replace A with Ah 2d4) If d.sub.1(i)=1 and d.sub.2(i)=1, replace A with Au 2d5) Return A (col.9 line 7 tocol.10 line 22).

As per Claim 5, the method comprises the following steps: 1) Masking of d: 1a) Express d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers 1b) Let (d.sub.1(t),d.sub.1(t-1), . . . ,d.sub.1(0)) and (d.sub.2(t),d.sub.2(t-1), . . . ,d.sub.2(0)) be the respective binary signed-digit representations for d.sub.1 and for d.sub.2 2) Exponentiation: 2a) Define (compute) the point R=s*P in G 2b) Initialize a register A with the neutral element of G 2c) For i from t down to 0, do the following: 2c1) Replace A with 2*A 2c2) If d.sub.1(i) is non-zero, replace A with A+d.sub.1(i)*P 2c3) If d.sub.2(i) is non-zero, replace A with A+d.sub.2(i)*R 2c4) Return A (col.9 line 7 tocol.11 line 46).

As per Claim 6, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer s and taking d.sub.2 equal to the default value of the integer division of d by s, and d.sub.1 equal to the remainder of said division (col.9 line 7 tocol.11 line 46).

As per Claim 7, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random

integer d.sub.1, setting s to the value 1, and taking d.sub.2 equal to the difference between d and d.sub.1 (col.9 line 7 tocol.11 line 46).

As per Claim 8, electronic component implementing the method according to claim 1 (col.12 line 39 tocol.12 line 6).

As per Claim 9, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer s and taking d.sub.2 equal to the default value of the integer division of d by s, and d.sub.1 equal to the remainder of said division (col.9 line 7 tocol.11 line 46).

As per Claim 10, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer s and taking d.sub.2 equal to the default value of the integer division of d by s, and d.sub.1 equal to the remainder of said division (col.9 line 7 tocol.11 line 46).

As per Claim 11, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer s and taking d.sub.2 equal to the default value of the integer division of d by s, and d.sub.1 equal to the remainder of said division (col.9 line 7 tocol.11 line 46).

As per Claim 12, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer s and taking d.sub.2 equal to the default value of the integer division of d by s, and d.sub.1 equal to the remainder of said division (col.9 line 7 tocol.11 line 46).

As per Claim 13, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random

integer d.sub.1, setting s to the value 1, and taking d.sub.2 equal to the difference between d and d.sub.1 (col.9 line 7 tocol.11 line 46).

As per Claim 14, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer d.sub.1, setting s to the value 1, and taking d.sub.2 equal to the difference between d and d.sub.1 (col.9 line 7 tocol.11 line 46).

As per Claim 15, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer d.sub.1, setting s to the value 1, and taking d.sub.2 equal to the difference between d and d.sub.1 (col.9 line 7 tocol.11 line 46).

As per Claim 16, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer d.sub.1, setting s to the value 1, and taking d.sub.2 equal to the difference between d and d.sub.1 (col.9 line 7 tocol.11 line 46).

As per Claim 17, the step of expressing the exponent d randomly in the form d=d.sub.2s+d.sub.1, where d.sub.1, d.sub.2, and s are integers, comprises choosing a random integer d.sub.1, setting s to the value 1, and taking d.sub.2 equal to the difference between d and d.sub.1 (col.9 line 7 tocol.11 line 46).

As per Claim 18, electronic component implementing the method according to claim 2 (col.12 line 39 tocol.12 line 6).

As per Claim 19, electronic component implementing the method according to claim 3 (col.12 line 39 tocol.12 line 6).

As per Claim 20, electronic component implementing the method according to claim 4 (col.12 line 39 tocol.12 line 6).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
November 30, 2009
/Syed Zia/
Primary Examiner, Art Unit 2431